

Configurazione del filtro dei contenuti Web con Cisco Umbrella in WAP571 o WAP571E

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare il filtro dei contenuti Web utilizzando Cisco Umbrella su un WAP571 o WAP571E.

Introduzione

Si è lavorato sodo per rendere operativa la rete. Certo, volete che rimanga così, ma gli hacker sono implacabili. Come proteggere la rete Una soluzione consiste nell'impostare il filtro dei contenuti Web. La funzionalità di filtro dei contenuti Web consente di fornire un accesso controllato a Internet mediante la configurazione di criteri e filtri. Consente di proteggere la rete bloccando siti Web dannosi o indesiderati.

Cisco Umbrella è una piattaforma di sicurezza cloud che fornisce la prima linea di difesa dalle minacce su Internet. Funge da gateway tra Internet e i sistemi e i dati per bloccare malware, botnet e phishing su qualsiasi porta, protocollo o applicazione.

Utilizzando un account Cisco Umbrella, l'integrazione intercetterà in modo trasparente (a livello di URL) le query DNS (Domain Name System) e le reindirizzerà a Umbrella. Il dispositivo verrà visualizzato nel dashboard Umbrella come dispositivo di rete per l'applicazione di criteri e la visualizzazione di report.

Per ulteriori informazioni su Cisco Umbrella, consultare i seguenti link:

[Cisco Umbrella in breve](#)

[Guida per l'utente di Cisco Umbrella](#)

[Procedura: Estensione di Cisco Umbrella per la protezione della rete wireless](#)

Dispositivi interessati

WAP571

WAP571E

Versione del software

- 1.1.0.3

Configurazione di Cisco Umbrella sul WAP

Passaggio 1. Accedere all'utility di configurazione Web di WAP immettendo il nome utente e la password. Il nome utente e la password predefiniti sono cisco/cisco. Se il nome utente o la password sono stati modificati, immettere le nuove credenziali. Fare clic su **Login**.

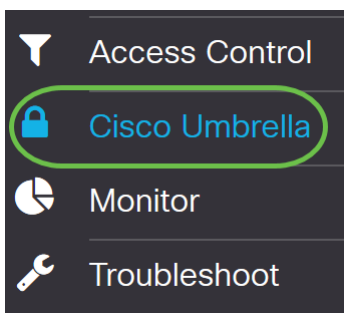


Wireless Access Point

A login form with a green border. At the top, the text "cisco" is entered in a text field, with a green circle containing the number "1" to its right. Below the text field is a password field containing ten black dots, with a green circle containing the number "2" to its right. Below the password field, the word "English" is displayed. At the bottom of the form is a blue button with the text "Login" in white, with a green circle containing the number "3" to its right.

Nota: In questo articolo, il protocollo WAP571E viene usato per dimostrare la configurazione di Cisco Umbrella. Le opzioni del menu possono variare leggermente a seconda del modello del dispositivo.

Passaggio 2. Scegliere **Cisco Umbrella**.



Passaggio 3. *Abilitare* Cisco Umbrella facendo clic sulla casella di controllo.

Cisco Umbrella

Cisco Umbrella is a cloud security platform that provide the first line of defense against
With an [Umbrella account](#), this integration will transparently intercept DNS queries and
This device will appear in the [Umbrella dashboard](#) as a network device for applying poli

Enable:

API Key: [?](#)

Secret: [?](#)

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

Passaggio 4. Per ottenere la chiave e il *segreto* API, accedere all'account [Cisco Umbrella](#) tramite *e-mail, nome utente e password*. Fare clic su **LOG IN**.



Cisco Umbrella

Email or Username

1

Password

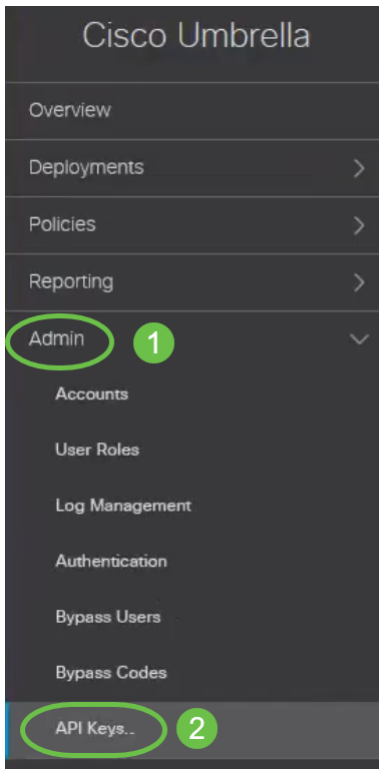
2

[Forgot password?](#) | [Single sign on](#)

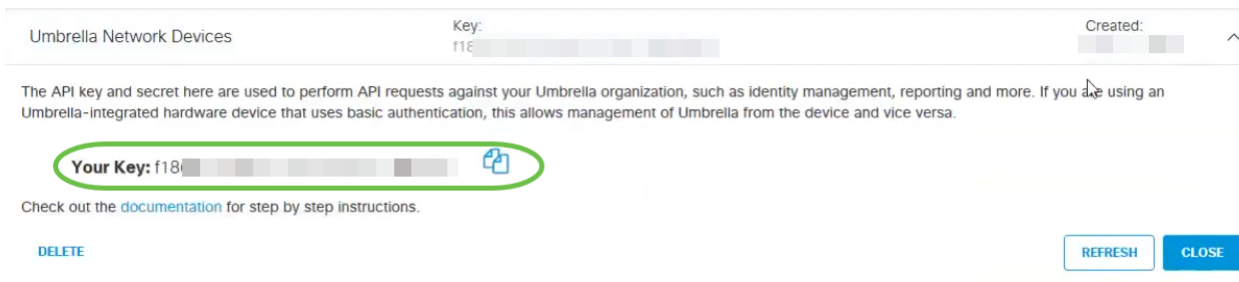
3

[Sign Up for a Free Trial](#)

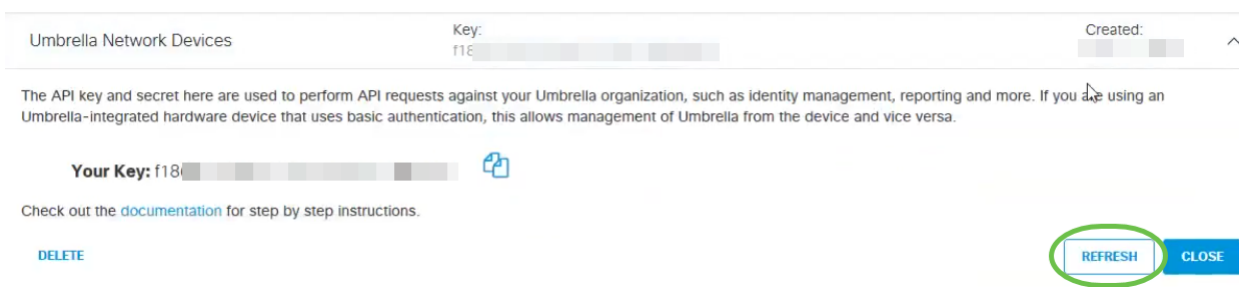
Passaggio 5. Passare ad **Admin** e richiedere una chiave API scegliendo **Chiavi API...** dal menu.



Nota: La prima volta che si richiede una chiave API, viene visualizzata solo la chiave, come mostrato di seguito.



Passaggio 6. Fare clic su **Refresh** per ottenere sia la chiave API che il segreto.



Nota: Quando si fa clic su *Aggiorna*, la chiave API cambia.

Passaggio 7. Copiare la *chiave* e il *segreto* generati.

Umbrella Network Devices

Key: dbb1 [redacted]

Created: [redacted]

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

Your Key: dbb1 [redacted]

Your Secret: 4e5 [redacted]

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

[DELETE](#) [REFRESH](#) [CLOSE](#)

Passaggio 8. Incollare la *chiave* e il *segreto* copiati dal passaggio 7 nei campi disponibili nella configurazione *Cisco Umbrella* del WAP.

Cisco Umbrella [Apply](#) [Cancel](#)

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key: 1

Secret: 2

Local Domains to Bypass (optional):

Device Tag (optional):

DNSEncrypt: Enable

Registration Status:

Passaggio 9. (Facoltativo) Immettere il nome di dominio considerato attendibile nel campo **Domini locali da ignorare (facoltativo)** e i pacchetti raggiungeranno la destinazione senza passare per Cisco Umbrella. Gli elementi dell'elenco devono essere separati da una virgola, mentre i domini possono includere caratteri jolly sotto forma di asterisco (*). Ad esempio: *.cisco.com.*

Cisco Umbrella [Apply](#) [Cancel](#)

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSEncrypt: Enable

Registration Status:

Nota: Questa operazione è necessaria per tutti i domini Intranet e per i domini DNS suddivisi in cui esistono server separati per le reti interne ed esterne.

Passaggio 10. (Facoltativo) Immettere un nome di tag nel campo **Tag dispositivo (facoltativo)** per

contrassegnare il dispositivo. Il *codice di matricola* descrive il dispositivo o una particolare origine assegnata al dispositivo. Garantire l'unicità del servizio all'interno dell'organizzazione.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

Nota: Qualsiasi modifica apportata ai campi *Secret*, *API Key* e *Device Tag* attiverà una nuova registrazione per creare un dispositivo di rete.

Passaggio 11. **DNSCrypt** viene utilizzato per proteggere (tramite crittografia) la comunicazione DNS tra un client DNS e un resolver DNS. Previene diversi tipi di attacchi DNS e snooping. È attivata per impostazione predefinita.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

Passaggio 12. Fare clic su **Applica** per applicare queste configurazioni.

Cisco Umbrella

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

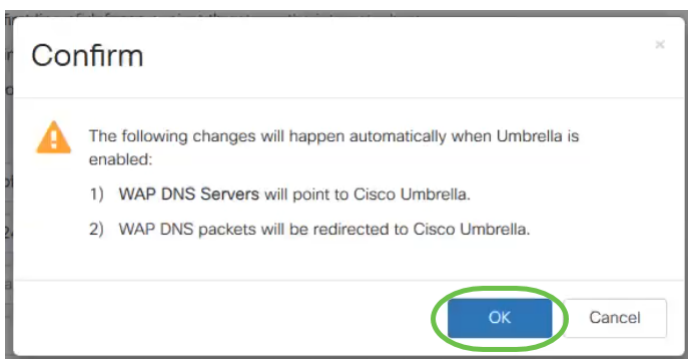
Device Tag (optional):

DNSCrypt: Enable

Registration Status:

Nota: Lo stato della registrazione è indicato nel campo *Stato registrazione*. Lo stato può essere *Riuscito*, *Registrazione* o *Non riuscito*.

Passaggio 13. Viene visualizzata una schermata di popup come mostrato di seguito. Fare clic su **OK** per confermare.



Verifica

C'è un modo divertente per controllare se il filtro del sito è abilitato. È sufficiente aprire un browser Web e immettere il seguente URL: www.internetbadguys.com. Non abbiate paura, questo è un sito di proprietà di Cisco a scopo di test e verifica.



Poiché il filtro dei siti Web è abilitato in WAP tramite Cisco Umbrella, si riceverà la seguente notifica. La rete wireless reindirizzerà la query DNS a Cisco Umbrella. A sua volta, Cisco Umbrella agisce come server DNS, proteggendo la rete e i suoi utenti.



This site is blocked.

www.internetbadguys.com

SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site www.internetbadguys.com has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this hostname was misclassified, please connect to the Cisco network and open a [case](#) with Infosec.

As a matter of good practice, you may check whether your browser or any component plugin is vulnerable by visiting browsercheck.qualys.com. The UID at the end of the browsercheck.qualys.com URL does not uniquely identify your machine to Qualys; it is a shared UID to group all requests originating from Cisco IP ranges.

[FAQ](#)

Conclusioni

È stato configurato e abilitato il filtro dei siti Web su un access point WAP571 o WAP571E con Cisco Umbrella.

Vuoi saperne di più? Guarda questi video relativi a Cisco Umbrella:

[Cisco Tech Talk: Protezione di una rete aziendale tramite i punti di accesso per piccole imprese Umbrella e Cisco](#)

[Cisco Tech Talk: Come ottenere un account Umbrella](#)

[Cisco Tech Talk: Impostazione di un criterio Umbrella](#)